



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/354,080

07/15/1999

MASSIMO BALESTRI

21197

4578

22852 7590 01/24/2008

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER  
LLP

901 NEW YORK AVENUE, NW  
WASHINGTON, DC 20001-4413

EXAMINER

KLIMACH, PAULA W

ART UNIT

PAPER NUMBER

2135

MAIL DATE

DELIVERY MODE

01/24/2008

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

## Office Action Summary

**Application No.**

09/354,080

**Applicant(s)**

BALESTRI ET AL.

**Examiner**

Paula W. Klimach

**Art Unit**

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 31 October 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-15 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-15 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- ☐ Notice of Informal Patent Application
- ☐ Other: \_\_\_\_\_

## **DETAILED ACTION**

### ***Response to Amendment***

This office action is in response to amendment filed on 10/31/07. The amendment filed on 10/31/07 have been entered and made of record. Therefore, presently pending claims are 1-15.

### ***Response to Arguments***

Applicant's arguments filed 10/31/07 have been fully considered and the newly cited reference is used to teach the newly amended limitation.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

1. **Claims 1-3, 5-6, 8-10, and 12-13** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al (6,157,719) and further in view of Sasaki (6,351,536), and further in view of Leppek (5,933,501).

*In reference to claims 1 and 8*, Wasilewski discloses a method for the controlled delivery of digital services to a user, wherein said services are identified by respective stream of encoded digital data emitted by said plurality providers (column 4 lines 20-23) and the user is provided with a receiver to receive said digital data streams from said plurality providers (Fig. 1), the receiver being selectively enabled to make use of determined services of a given provider

Art Unit: 2135

(column 4 lines 41-50). The system includes a single removable user unit to be associated to said receiver for enabling the use of respective determined services of the provider (Fig.12 in combination with column 21 lines 15-27). An identifying code is incorporated into the digital data stream for the user to enabled to receive said determined services (column 4 line 64 to column 5 line 13). The single removable user unit is associated to a processing function capable of security functions by exploiting said identifying code to enable the receiver of the user to make use of said determined services (column 5 lines 23-27).

Wasilewski does not expressly disclose incorporating into the digital data streams respective enabling algorithm of at least two of the plurality of providers into the user unit of at least one of the selective users based on the respective identifying codes for enabling the at least one of the selective users to make use of said respective determined services.

Sasaki discloses a system and method wherein the ciphertext, together with a key generation program in a public key cryptosystem, is transmitted from the transmitter to the receiver (abstract). The method and system of Sasaki comprises incorporating into the digital data streams respective enabling algorithm (column 8 lines 27-41) of at least two of the plurality of providers (column 5 lines 35-45) into the user unit of at least one of the selective users (column 5 lines 35-45) based on the respective identifying codes for enabling the at least one of the selective users to make use of said respective determined services (column 6 lines 10-15).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to transmit the enabling algorithm as in the system of Sasaki in the system of Wasilewski. One of ordinary skill in the art would have been motivated to do this because the

Art Unit: 2135

method for checking the second device makes it possible to prevent second device from acquiring the means to decipher the ciphertext unless the addresses coincide with each other.

Although Sasaki teaches a system and method Sasaki does not expressly disclose a system and method wherein the enabling algorithm is selectively loaded.

Leppek teaches a system and method wherein the enabling algorithm is selectively loaded wherein the access code indicate the selected algorithm (column 4 lines 7-23).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to selectively load the enablement algorithm as in Leppek in the system of Sasaki. One of ordinary skill in the art would have been motivated to do this because it would decrease the discernible encryption footprint (column 2 lines 25-38).

*In reference to claims 2 and 9* wherein the single removable user unit is configured as a movable processing support uniquely assigned to the user (column 21 lines 11-14).

*In reference to claims 3 and 10*, wherein the single removable user unit configured as a smart card (column 21 lines 11-14).

*In reference to claims 6 and 13* wherein the enabling algorithm is incorporated into a stream of private data within said data streams (Sasaki Fig. 4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the servers of Wasilewski to create the upgrade or modify cryptographic algorithm by an authorized entity as in Sasaki. One of ordinary skill in the art would have been motivated to do this because it may be possible to ease export restrictions and allow regional licenses for such modifiable cryptographic devices which would greatly reduce the costs associated with heightened regulated supervision.

*In reference to claims 5 and 12*, Wasilewski teaches of a system for conditional access where the service provider sends data streams in MPEG format, column 18, lines 32-35. The receiver extracts the EMM message from the data stream, column 5 lines 9-13, where it stores the information from the EMM, therefore must extract the information. It uses a control word that includes authorization information from the EMM, therefore it interprets the identification code contained in the EMM message, column 4 lines 52-58. Wasilewski teaches of an algorithm that generates the control word, which is used to decrypt the information, if the subscriber is entitled to watch the program, thus an enabling algorithm that is on the basis of the authentication information (identification code). Wasilewski teaches a smart card and therefore a removable algorithm

2. **Claims 7 and 14** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski and Sasaki and Leppek as applied to claims 3 and 13 above, and further in view of Spies (6, 055, 314).

Wasilewski and Sasaki and Leppek do not expressly teach the processor transmitting information about the delivery of the service itself.

The system described by Spies can be activated by the user unit to transmit information about the confirmation of the purchase request, thus about the delivery of the service.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to send information about the purchase as in Spies in the system of Wasilewski. One of ordinary skill in the art would have been motivated to do this because it would enable the system to carry out error checking and correct information that was not received correctly.

Art Unit: 2135

3. **Claims 4 and 11** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski and Sasaki and Leppek as applied to claims 1 and 8 above, and further in view of Jones et al (5, 623, 637).

Wasilewski and Sasaki and Leppek do not expressly disclose a system with a trusted middleware function in the reception means and a trusted middleware function in the dynamic part.

Jones discloses an embodiment of a system where trusted software carries out an authentication algorithm on the IC card (smart card) as well as on the host, column 8 line 13-34.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to have a trusted middleware function in the static part (the host in the Jones system) and have a middleware in that dynamic part (the smart card). One of ordinary skill in the art would have been motivated to do this because the removable card allows data stored on the card to be made immediately available to the connected host computer, Jones column 2 lines 23-29.

4. **Claim 15** is rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski and Sasaki and Leppek as applied to claim 8 above, and further in view of Kaplan et al (6,141,339).

Wasilewski, Sasaki, and Leppek do not teach the use of Java cards.

Kaplan teaches of Java cards used to receive applets from service nodes, column 5 lines 59-61. At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Java cards for the user unit. One of ordinary skill in the art would have

Art Unit: 2135

been motivated to do this because Java applets provide the intelligence to support features, Kaplan column 5 lines 61-65.

### ***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

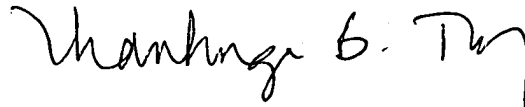
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.



Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK  
Saturday, January 19, 2008



THANHNGA TRUONG  
PRIMARY EXAMINER